ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●イベント管理等サービス「Peatix」に不正アクセス…最大677万件の個人情報流出

https://www.itmedia.co.jp/news/articles/2011/18/news066.html
https://peatix.com/event/1721625

このニュースをザックリ言うと･･･

- 11月17日(日本時間)、イベント管理・電子チケット販売サイト「Peatix」の運営元より、同サイトが不正アクセスを受け、ユーザーのアカウント情報が流出したと発表されました。

- 被害を受けた可能性があるのは、Peatixユーザーの氏名・メールアドレスおよび暗号化されたパスワード等最大677万件とされています(クレジットカード・銀行口座情報等決済関連情報やイベント参加履歴・アンケート回答データ・住所・電話番号等は流出は確認されていないとのことです)。

- 不正アクセスは10月16日～17日に発生したとされ、運営元では11月15日より全ユーザーに対しパスワードの変更等の対応を呼び掛けています。

AUS便りからの所感等

- 攻撃者が集うWebサイトに流出したデータがアップロードされた、さらにはパスワードの暗号化が解読されたという情報もあり、流出データを悪用した大規模な「リスト型攻撃」も既に発生している恐れがあります(ただし、Twitter等SNSとの連携で登録・ログインしているユーザーについてはパスワードは保持していないとのことです)。

- 近年、パスワードの設定に関して、サービス毎に異なる、推測されにくいパスワードを設定することが推奨されていますが、もし使用しているサービスから流出したのと同じパスワードを他のサービスで使い回していた場合、リスト型攻撃のターゲットとなり得る上、他のサービスのパスワードを後から変更する手間も発生することに注意が必要です。

- Peatixは多種多様なイベント、また一部の自治体によるプレミアム商品券の販売等にも利用され、利用者によってはお知らせメールが届くまでサイトに登録したことを覚えていなかったという人も散見されており、例えばパスワード管理ツール等も用いて、自分が登録したWebサービスの管理を普段から行っておくことは、万が一こういった事態が発生した場合にもパスワードの変更等迅速な対応ができるようにするため、重要と言えます。

ITmedia NEWS

電子チケット販売「Peatix」に不正アクセス　最大677万件の個人情報流出

2020年11月18日 10時22分 公開　[岡田有花，ITmedia]

印刷　見る　Share　B! 19

日系ベンチャーの米Peatixは11月17日、電子チケット販売プラットフォーム「Peatix」（ピーティックス）が10月に不正アクセスを受け、ユーザーの氏名やメールアドレス、暗号化されたパスワード最大677万件が引き出されていたと発表した。被害拡大を防ぐため11月15日から、全ユーザーに対して、パスワード再設定を依頼している。

同サービスは、一部の自治体でプレミアム商品券の販売にも使われており、波紋が広がりそうだ。

Peatix

<不正アクセスの経緯>

11月9日に弊社保有のお客様の個人情報が引き出されている可能性があることを認識し、外部の調査会社による調査を行った結果、10月16日から10月17日にかけて発生した不正アクセスにより、お客様の個人情報を含むお客様情報（氏名、メールアドレス、暗号化されたパスワードなど）が最大677万件引き出された事実が判明しました。その他詳細は現在も調査中であり、新たな事実が判明次第早急に公表させていただきます。

<不正に引き出されたお客様情報>

Peatixに登録されているお客様の以下の情報が不正に引き出されたことを確認しております。

- 氏名
- アカウント登録メールアドレス
- 暗号化されたパスワード
- アカウント表示名
- 言語設定
- アカウントが作成された国
- タイムゾーン

なお、クレジットカード情報および金融機関口座情報などの決済関連情報ならびにイベント参加履歴、参加者向けのアンケートフォーム機能で取得したデータ、住所、電話番号などの情報が引き出された事実は確認されておりません。

●仮想通貨取引所「Liquid」のドメイン名管理サービスに不正アクセス

https://scan.netsecurity.ne.jp/article/2020/11/17/44822.html
https://blog.liquid.com/ja/20201118-important-notice-2
https://nextmoney.jp/?p=36260

このニュースをザックリ言うと･･･

- 11月16日(日本時間)、仮想通貨(暗号資産)取引所「Liquid」運営元のQUOINE社より、同社利用のドメイン名の情報がサイバー攻撃で一時改ざんされていたと発表されました。

- ドメイン名登録サービス「GoDaddy」上における同社のアカウントが不正アクセスを受けたことによるもので、これにより、11月13日～14日に送られた問合せメールについて、第三者が不正に取得できる状態になっていたとのことです。

- ユーザーのAPIトークンおよび本人確認手続において送信された証明書等の画像についても攻撃者が取得可能だった可能性もあるとする一方、ユーザーから預かった資産への影響はないとのことです。

AUS便りからの所感

- 6月には国内のドメイン名登録サービスが不正アクセスを受け、「Coincheck」等複数の仮想通貨取引所が問合せメールを奪取される等の被害を受けており(AUS便り 2020/06/08号参照)、今回もGoDaddyにドメイン名情報を登録していた他の取引所がQUOINE社と同様の攻撃を受けたとの情報があります。

- ドメイン名の管理権限の奪取は、情報の改ざんによる偽のサーバーへの誘導や、SSL証明書等の不正な取得に繋がる他、ドメイン名自体の乗っ取り・他の登録サービスへの勝手な移管の実施等を引き起こされる恐れもありますので、アカウントが不正ログインされないよう強力なパスワードを設定すること、ログインや設定変更等における通知メールを確実に受信できる設定・体制を整えること、ドメイン名自体にも不正な移管防止のためのレジストリロックを設定する等、各種対策をとるよう心掛けてください。

ScanNetSecurity

仮想通貨取引所「Liquid」に不正アクセス、お問い合わせメール内容が流出

暗号資産・仮想通貨取引所「Liquid」を運営するQUOINE株式会社は11月16日、同社が利用するドメイン登録サービス「GoDaddy」内の同社アカウントにて不正アクセスを確認したと発表した。

暗号資産・仮想通貨取引所「Liquid」を運営するQUOINE株式会社は11月16日、同社が利用するドメイン登録サービス「GoDaddy」内の同社アカウントにて不正アクセスを確認したと発表した。

これは11月13日午前5時58分頃に、「GoDaddy」内の同社アカウントにて第三者によるドメイン登録情報の変更を確認、その後、同社テクノロジー部門で社内調査を行ったところ、2020年11月13日から11月14日の期間に顧客から問い合わせのあった一部のメールについて、第三者が不正に取得できる状態であったことが判明したというもの。


トップページ


リリース（当社利用のドメイン登録サービスにおける不正アクセスについて（第一報））


リリース（発生事象）


リリース（当社での対応について）

● UCS・アプラス・ポケットカード…クレジットカード各社を騙るフィッシング相次ぐ

https://www.antiphishing.jp/news/alert/

このニュースをザックリ言うと･･･

- 11月9日(日本時間)以降、クレジットカード各社を騙るフィッシングについて、被害を受けた各社およびフィッシング対策協議会より相次いで注意喚起が出されています。

- 9日に発表されたのはUCSカード(ユニー系列)を騙るもので、件名が「UCSカード株式会社から緊急のご連絡」で、第三者によるカード不正使用の可能性があるとして、カード情報・個人情報を詐取する偽サイトに誘導するものとなっています。

- 同16日にはアプラス(新生銀行系)を騙るフィッシングの注意喚起が発表されており、件名は「<重要>【APLUS】ご利用確認のお願い」「【新生銀行カード】ご利用確認」「【NETstationAPLUS】新生銀行カード利用確認」が確認され、カードの利用を一部制限したと偽って偽サイトに誘導する模様です。

- さらに20日にはポケットカード(ファミマTカード等)を騙るフィッシングの存在が発表され、件名は「<重要>【POCKETCARD】ご利用確認のお願い」で、やはりカードの一部利用を制限したとして偽サイトに誘導するものが示されています。

AUS便りからの所感

フィッシング対策協議会 Council of Anti-Phishing Japan

- いずれのフィッシングも「第三者によるカード不正利用防止のためモニタリングを行っている」「お客様のカードで不正利用の可能性があり、一部利用を制限している」としてフィッシングサイトに誘導し、カード情報(番号・名義・有効期限・セキュリティコード)の他、生年月日・電話番号・登録口座番号等を詐取するシナリオとみられます。

- 対策協議会や各社からの発表にもある通り、このようなフィッシングサイトで決して情報を入力しないこと、また普段からの自衛のため、ブラウザーのブックマーク(あるいは公式スマホアプリのメニュー)からサイトにアクセスすることが重要です。

- 一方で、各社からの本物の注意喚起メールにおいても、一部には「注意喚起の詳細」へのリンクを記載しているものが見受けられ、攻撃者がこれを模倣したフィッシングメールを作成する恐れもあることから、顧客をフィッシングから保護する意味では、ここでも前述のようなブックマーク等からのアクセスが呼び掛けられるようになることを期待したいものです。


ポケットカードをかたるフィッシング (2020/11/20)

緊急情報

2020年11月20日

概要

ポケットカードをかたるフィッシングの報告を受けています。

メールの件名

＜重要＞【POCKETCARD】ご利用確認のお願い

詳細内容

ポケットカードをかたるフィッシングの報告を受けています。

1. 2020/11/20 11:00 現在フィッシングサイトは稼働中であり、JPCERT/CC にサイト 閉鎖のための調査を依頼中です。模倣のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。

2. このようなフィッシングサイトにて、ログイン ID、パスワード、個人情報（氏名、生年月日、ご登録電話番号）、クレジットカード情報（カード番号、有効期限、セキュリティコード）、口座番号等を絶対に入力しないように、ご注意ください。

3. 日頃からサービスへのログインする際は、メールや SMS 内のリンクではなく、いつも利用しているスマートフォンの公式アプリやブラウザのブックマークなどからアクセスするよう、心がけてください。

4. 模倣のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

【参考情報】
ポケットカードを騙るなりすましメールにご注意ください
https://www.pocketcard.co.jp/news/detail.php?id=316

サイトのURL

https://www.pocketcard.co.jp.●●●●.com/

上記以外のドメイン名、URL も使われている可能性があります。

メール本文

＋拡大する

サイト